A-F

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No. APP 1365

In Re Application Of: **David Marples et al**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/052,094	01/18/2002	DUONG, Oanh L.	09941	2155	5824

Invention: **Initiating Connections Through Firewalls and Network Address Translators**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:

January 19, 2006

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 021822. I have enclosed a duplicate copy of this sheet.

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **February 7, 2006**

James W. Falk (Reg. No. 16154)
Telcordia Technologies, Inc.
One Telcordia Drive 5G116
Piscataway, NJ 08854-4157
Telephone (732) 699-4465

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

February 7, 2006
(Date)

Signature of Person Mailing Correspondence

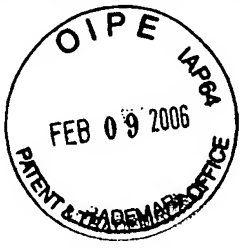
Vivian Austin

Typed or Printed Name of Person Mailing Correspondence

cc:

AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Appl. No.	:	10/052,094	Confirmation No. 5824
Applicants	:	David Marples et al	
Filed	:	January 18, 2002	
TC/A.U.	:	2155	
Examiner	:	Oanh L. Duong	
Docket No.	:	APP 1365	
Customer No.	:	09941	

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

This appeal arises from the Examiner's Final Rejection dated October 25, 2005, of Claims 19, 20, and 21.

(i) Real Party in Interest

The real parties in interest are appellants David Marples, Stanley Moyer, and Christian Huitema and Telcordia Technologies, Inc., appellants' assignee and employer with respect to the invention of this application, the assignment having been recorded on May 28, 2002, Reel/Frame 012939/0735.

(ii) Related Appeals and Interferences

To the best of knowledge of appellants, appellants' legal representative, and appellants' assignee, there are no other appeals or interferences which will directly affect of be directly affected or have a bearing on the Board's decision in the pending appeal.

(iii) Status of Claims

In this application, claims 1 to 15 were originally presented. These claims were rejected in an Office Action of October30, 2003, as unpatentable, 35 USC 103(a), over Poier et al patent publication US 2002/0124090 in view of Murakawa patent publication 2001/0020273. By an Amendment dated January 30, 2004, claims 1, 8, and 12 were Amended.

In a Final Office Action of April 23, 2004, claims 1-4, 6-10, and 12-15 were rejected, 35 USC 103(a), as unpatentable over Murakawa patent publication US 2001/0020273 in view of Calhoun patent 6,463,475). Claims 5, 11, and 15 were rejected, 35 USC 103a), as unpatenable over Murakawa in view of Calhoun in further view of Poier. In an Amendment dated July 22, 2004, in response to this Final Rejection appellants proposed to amend claims 1, 6, 8, 10, and 12 and to cancel claims 2-5, 7, 9, 11, and 13-15. This Amendment was not entered, by the Advisory Action of August 16, 2004, but was then resubmitted with a Request for Continued Examination, dated September 14, 2004.

In an Office Action dated October 21, 2004, claims 1, 6, 819, and 12 were again rejected as unpatentable over Murakawa in view of Calhoun. By an Amendment dated November 3, 2004, claims 1, 6, 8, and 12 were canceled and replaced by new claims 16 and 17, with claim 10 being amended to depend from new claim 16.

Claim 16, 17, and 10 were then rejected in a Final Office Action dated March 9, 2009, as unpatentable over Calhoun in view of Murakawa. In response thereto appellants proposed, in an Amendment of March 31, 2005, to cancel these claims and replace them with new claims 18 and 19. This Amendment, however, was refused entry by the Advisory Action of April 15, 2005, in response to which appellants filed a Request for Continued Examination dated May 12, 2005, together with an Amendment dated May 12, 2005, resubmitting new claims 18 and 19.

In an Office Action dated June 17, 2005, claims 18 and 19 we first rejected, 35 USC 112, first paragaph, and were then rejected, 35 USC 102(b), as anticipated by McCann et al patent 6,052,725. By an Amendment dated August 9, 2005, claim 18 was cancelled, claim 19 amended, and new claims 20 and 21 added.

This resulted in the Final Rejection being appealed from and in which claims 19 and 20 were, for the first time, rejected, 35 USC 103(a) as unpatentable over McCann et al in view of Tuomenoksa et al patent publication 2002/0023210 and further in view of Calhoun. Claim 21 was rejected, 35 USC 103 (a), as being unpatentable over just McCann et al in view of Tuomenoksa et al.

(iv) Status of Amendment

No Amendment was filed after the Final Rejection being appealed from.

(v) Summary of Claimed Subject Matter

Claims 19 and 21 of the appealed claims are both independent claims. Both of these claims recite the underlying combination of appellants' invention including a security blocking apparatus or firewall 222 which separates a first communication device 220 from a plurality of second communication devices 240, 242, with a public network 112 between the first and second devices. Crucial to appellants' invention is a secure hub 200 which is described, inter alia, at page 3, line 23 et seq of appellants' specification. The secure hub includes network interfaces 206, routing and switching functions 202 and means 204, together with the first device 220, to establish a virtual pipe between the first device and the secure hub. The secure hub, using 204, assigns, from an available IP address pool 212 assigned to the hub a secondary IP address 230 to the first device and associates this address with the pipe. (page 3, lines 30-32)

The secure hub 220, when a communication 228 from a second device is routed by the public network 112 and addressed to the first device, will route/tunnel, using 202, the communication over the pipe and through the firewall to the first device (page 4, lines7-9).

(vi) Grounds of Rejection to be Reviewed on Appeal

In the Final Rejection being appealed from the Examiner (1) has rejected claims 19 and 20, 35 USC 103(a), as unpatentabale over McCann et al patent 6,052,725 (hereinafter McCann) in view of Tumenoksa et al patent publication US 2002/0023210 (hereinafter Tuomenoksa) and further in view of Calhoun patent 6,463,475 and (2) rejected claim 21 as unpatentable, 35 USC 103(a) over McCann in view of Tuomenoksa.

The issues presented by this appeal accordingly are:

(a) Whether one of ordinary skill in the art would be motivated to use the tunnel procedures of Tuomenoksa to enable communications between different gateways in a system with firewalls somehow in the routing arrangements of McCann and

(b) Whether such a hypothetical combination, including the plurality tunnel connections of Calhoun, would in any way resemble or suggest appellants' claimed apparatus as set forth in claims 19, 20 and 21.

(vii) Argument

Appellants' invention is directed to the problem of allowing a private communication device which has an primary IP address and is protected from calls to that primary IP address by blocking apparatus, such as a firewall, between it and the public network nevertheless to receive certain communications originating from the external side of the firewall without having to reconfigure the firewall or to decrease the security the private communication device receives. As is known, firewalls are typically configured to allow outgoing calls but inhibit or block incoming calls. This problem in the prior art of utilizing the firewall or other blocking apparatus while still allowing some communications is described in appellants' specification in the section "Description of the Background" at page 1, line 11 to page 2, line 3.

Appellants' invention resolves this problem by a combination of elements which gives the private device behind the firewall a second network appearance to which external devices in front can address communications. Critical to appellants' invention is thus the concept of a second IP address for the private device and a secure hub. In accordance with appellants' invention the secure hub, which includes both switching and routing functions, interfaces with the public network, establishes a tunneling virtual pipe, assigns a second IP address to the private communication device, and associates that second IP address with the single virtual pipe.

The use of virtual pipes to by-pass firewalls is, itself, known in the prior art to appellants' invention, but such use has not involved the concept of assigning a second address to a private communication device or the use of the secure hub which attains the various functions requisite to the use of that second address.

The primary reference relied upon by the Examiner is McCann. Prior to the Final Rejection being appealed from, the Examiner was asserting, erroneously, that McCann disclosed firewalls and the by-passing of such firewalls. The Examiner now admits that such is not the case. What McCann discloses is the use of routers to improve dynamic IP addressing to allow for the use of both local and non-local dynamic IP addressing. The problem to which McCann is addressed involves the fact that " because dynamic addressing works only if an unassigned local address is available, the user must wait until one becomes available in the region or retry at a later time." (column 1, lines 50-53). McCann does not in any way use tunnels to by-pass access blocking apparatus. McCann's teaching is how to assign a non-local dynamic address which is transmitted to a remote visitor database together with a remote router's IP address. (column 7, lines 1-9) The non-local dynamic address is not a secondary address for a private communication user, as in appellants' invention, because, to quote the paragraph relied upon by the Examiner, "Once the non-local dynamic IP address from the remote pool of non-local dynamic addresses 40 has been assigned from the remote network 32 to the communication device 16, the non-local dynamic address is used for the duration of the communication session between the communication device 16 and the IP network 14." (column 7, line 66 - column 8, line 4)

In the Final Rejection being appealed from the Examiner asserts that, with respect to claim 21, the McCann router 34 is a secure hub and also with respect to claims 19 and 20, refers to McCann column 7, lines 22-23 for the secure hub. That sentence reads "The remote router 34 establishes a communication 56 with the IP network 14." Central to this appeal is the Examiner's continual erroneous insistence that router 34 is and can perform all of the functions of appellants' secure hub. However, McCann is perfectly clear in describing what his router 34 is and does. Thus McCann states that the remote router 34 "receives communications from other networks and determines the paths the communications should follow." (column 5, lines 33-35). The McCann router 34 does not establish a single virtual pipe between the private communication device behind a firewall and itself, nor does it provide for tunneling over the virtual pipe to bypass the firewall. Further, the fact that in McCann there is a remote pool of non-local dynamic IP addresses is irrelevant to appellants' secure hub and the assignment of a secondary incoming address for the private communication device behind the firewall.

Tuomenoksa, which was newly cited by the Examiner for the first time in the Final Rejection, is concerned with bypassing firewalls, but in an entirely different type of communication setting involving the implementation of virtual private networks and not, as with appellants' invention, the communication to a single specific private user. The Examiner has specifically referred to page 15, paragraphs 155 and 156, which need to be considered together with the diagrams of Figs. 6A and 6B and the flow chart of Fig. 13. The lack of relevance to appellants' invention is readily apparent from the description of what Tuomenoksa refers to as a "Hairpin", namely the proxy module 613 in the network operations center 610. This Hairpin enables a tunnel between two gateways through the proxy module. Note that this arrangement occurs in the situation, described with reference to Fig. 13, that the first gateway and the destination gateway are not accessible because both are behind firewalls.

The teaching of Calhoun of "routing and switching functionalities", at column 4, lines 35-59, is so general with respect to Calhoun's tunnel switching across or through a network as to be of no help to one of ordinary skill in the art when considering the disparate, and conflicting teachings, of McCann and Tuomenoksa. Calhoun involves tunnel network connections, as known in the art, that allow a user to access a destination network via an intermediate network such as the public Internet. (see column 1, lines 25-27). His disclosure and teaching are directed to improving such arrangements by providing a number of additional abilities, namely, determining the appropriate destination for switching incoming tunnel connections (column 2, lines 23-25), imposing security verification on users before initiating the switched tunnel connection (column 2, lines 33-35), providing load balancing (column 2, line 49), and allowing for the bundling together of a plurality of tunnels (column 2, lines 63-65). None of this would suggest to one skilled in the art that Calhoun should or could be combined in some way with McCann and Tuomenoksa to render appellants' invention obvious.

Finally, appellants submit that these references, individually or in combination, are not directed to the problem solved by appellants' invention. Further, appellants

submit that there is nothing in the references to lead or to suggest to one skilled in the art that they may be combined. In fact, appellants dispute that any such combination is possible since any such combination would be contrary to and would defeat the purposes and operations of each of the references.

(viii) Claims Appendix

Claims 19, 20, and 21 are set forth in the attached Appendix.

(ix) and (x) Evidence and related proceedings appendices.

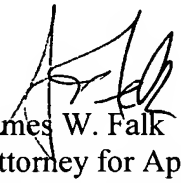
There is no evidence to be presented nor are there any related proceedings.

(xi) Conclusion

For the reasons set forth above, it is submitted that the Final Rejection of claims 19, 20, and 21 is in error. Reversal of this rejection is therefore respectfully requested.

The Commissioner is authorized to charge Deposit Account 021822 to cover the fees for this Appeal Brief.

Respectfully submitted,



James W. Falk
Attorney for Appellants
Reg. No. 16,154
(732) 699-4465

Enclosed
Two Additional Copies of this Appeal Brief

Telcordia Technologies, Inc.
One Telcordia Drive 5G116
Piscataway, NJ 08854-4157

Appendix

CLAIMS ON APPEAL

Claim 19: A communication system comprising

a first communication device, said first communication device having a primary IP address,

a plurality of second communication devices connectable to a public network,

security access blocking apparatus that provides the first communication device access to the public network and separates the first and second communication devices, said security blocking apparatus normally allowing outgoing communication from said first communication device but normally disallowing incoming communication to said first communication device, and

a secure hub including routing and switching functions, interfaces to the public network, means in response to the first communication device for establishing a single virtual pipe between said secure hub and the first communication device for tunneling communication and bypassing said security access blocking apparatus, and means for assigning a secondary IP address to said first communication device and associating said secondary IP address with said established single virtual pipe.

Claim 20: The communication system in accordance with claim 19 further including means defining a pool of available IP addresses, said secure hub obtaining said secondary IP address from said IP address defining pool means.

Claim 21: A communication system comprising

a firewall,

a first communication device behind said firewall and having a primary IP address, said firewall normally allowing outgoing communications from said first communication device but normally disallowing incoming communications to said first communication device,

a public network,

a plurality of second communication devices connectable through said public network, said public network being between said second communication devices and said first communication device,

a secure hub, said secure hub including

interfaces connecting said secure hub to the public network,

means in response to the first communication device for establishing a single virtual pipe between the first communication device and said secure hub,

a pool of available IP addresses, and

means for assigning an IP address from said pool to the established single virtual pipe, whereby the first communication device has a secondary IP address,

means for routing communications from any of the second communication devices and addressed to the first communication device to the established virtual pipe utilizing the assigned secondary IP address; and

means for tunneling said communications over the established virtual pipe to the first communication device thereby bypassing said firewall.